Journal of Engineering, Electrical and Informatics

E- ISSN: 2809-8706
P- ISSN: 2810-0557

Research Article

Hybrid Federated Ensemble Learning Approach for Real-Time Distributed DDoS Detection in IIoT Edge Computing Environment

Danang Danang [1*], Siswanto Siswanto[2], Widya Aryani[3], Priyo Wibowo[4]

[1-3] Universitas Ilmu Komputer dan Teknologi,Indonesia; email: danang150787@gmail.com

[4]Politeknik Katolik Mangunwijaya

Corresponding Author: Danang Danang

Abstract: Development rapid from the Industrial Internet of Things (IIoT) and edge computing have revolutionize modern industry through distributed data processing with latency low . However , progress this also enlarges risk security cyber , in particular Distributed Denial of Service (DDoS) attacks can to disable operation industry that is critical . System Detection Conventional Intrusion (IDS) own limitations in matter scalability , data privacy , and capabilities generalization to environment Heterogeneous IIoT . For answer challenge said , research This propose A framework Hybrid Federated–Ensemble Learning (FL–EL) work to improve efficiency detection real -time DDoS attacks on networks IIoT edge -based . This model utilizing the Edge -IIoTset dataset which reflects pattern Then cross real in system industry . Federated learning is used For train the model collaborative across multiple edge nodes without need move data to center , so that guard data privacy . Each node performs training local using the basic model such as Random Forest (RF), XGBoost , and Support Vector Machine (SVM). Then , the central server do aggregation use ensemble techniques such as soft voting and stacking. The preprocessing process includes SMOTE technique and Z-score normalization for handle imbalance class and improve performance .Evaluation results show that This FL–EL hybrid approach capable reach performance high (F1-score > 99.5%) and significantly significant reduce level error positive as well as burden communication , compared with approach centralized . Framework this also shows ability detection fast with latency low , making it suitable For implementation in the system IIoT that requires resilience time real . Development advanced will covers Explainable AI integration for model interpretation and blockchain for secure and transparent logging .

Keywords: DDoS Detection , Edge Computing, Ensemble Learning, Federated Learning, Industrial IoT

1. Introduction

of Things technology Things (IIoT) in the Industry 4.0 ecosystem has created high connectivity between smart devices and automation systems in the manufacturing, healthcare, transportation, and critical infrastructure sectors. IIoT enables real -time monitoring and decision-making through distributed sensors, actuators , and communication systems. However, the growth of this infrastructure also creates an attack surface surface) which is wider, especially against Distributed attacks Denial of Service (DDoS) which aims to paralyze the system through excessive traffic (Alam et al. , 2024; Priyadarshini & Barik, 2022; Mr et et al. , 2020; Sumathi et et al. , 2022).

Traditional security systems such as Intrusion Signature-based Detection Systems (IDS) have limitations in identifying new, unknown attacks, especially in edge environments. computing that has limited resources and is decentralized. Signature-based IDS are unable to adapt to the ever-evolving variety of DDoS attack patterns and are often hidden in normal traffic (Potluri et et al. , 2020; Amjad et al. , 2019; Khempetch & Wuttidittachotti , 2021). Several studies have proposed deep learning-based approaches learning such as Elman Neural Network (Varma et al., 2023), Recurrent Neural Networks (RNN) (Ur Rehman et al. ,2021), and feed-forward DNN (Cil et al., 2021), but most of them are still centralized and have not been optimized for edge environments.

Received: 28,June,2025;
Revised: 25,July,2025;
Received: 30,July,2025;
Published: 04,August,2025;
Current version: 04,August,2025

Recent studies have shown the effectiveness of ensemble and deep learning approaches for attack detection, such as the combination of RNN and CNN models (Songa & Karri, 2023; Balasubramaniam et et al., 2023; Agarwal et al., 2022). However, until now no approach has been found that specifically integrates Federated Learning (FL) and Ensembles Learning (EL) to detect DDoS attacks collaboratively and in real- time in edge environments . FL enables distributed model training without the need to move raw data, thus ensuring privacy and communication efficiency (Alghazzawi et al. , 2021; Dinh & Park, 2021), while EL is known to improve prediction accuracy through the aggregation of multiple classification models (Katiravan & SP, 2024; Kushwah & Ranga , 2021; Velliangiri et et al. , 2021).

Taking these research gaps into consideration, it is important to design a framework Federated Ensemble Learning that can be implemented efficiently at the edge network . This framework is expected to be able to detect DDoS collaboratively, in real- time , and maintain data integrity and system efficiency. This study aims to fill this gap while providing a significant contribution to strengthening IIoT security systems in the digital era (Elman, 1990; Sharafaldin et al. , 2019). The main objective from approach This is :

1. Increase accuracy and sensitivity detection DDoS attack with combining local models ;
2. Guard data privacy with model training federative ;
3. Give adaptive and scalable solutions For applied to the system IIoT based on edge computing.

Following is an architectural diagram Hybrid Federated–Ensemble Learning system for DDoS detection on Edge- IIoT

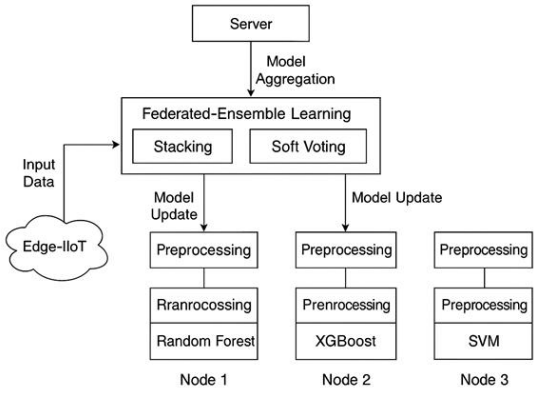

Figure 1 system architecture diagram

This study using the Edge -IIoTset dataset, which is wide considered as representation realistic from Then cross network IIoT with various scenario attacks, including DDoS attacks such as HTTP flood, ICMP flood, TCP-SYN flood, and UDP flood.

2.Theoretical Study

Ensemble Learning is a machine learning approach that combines predictions from multiple base models to improve accuracy and robustness . In the context of IIoT security , ensemble learning has been shown to be effective in detecting DDoS attacks , especially when combined with feature selection and deep learning (Songa & Karri , 2023; Balasubramaniam et al. , 2023). Models such as Random Forest , Gradient Boosting, and Voting Classifier have been used to reduce false positives and increase the sensitivity of the system in classifying malicious traffic (Agarwal et al.,2022; Cil et al., 2021). Several studies have also developed ensemble -RNN and ensemble -DNN as voting-based architectures for DDoS detection on traffic. IIoT (Katiravan & SP, 2024; Velliangiri et et al. , 2021)

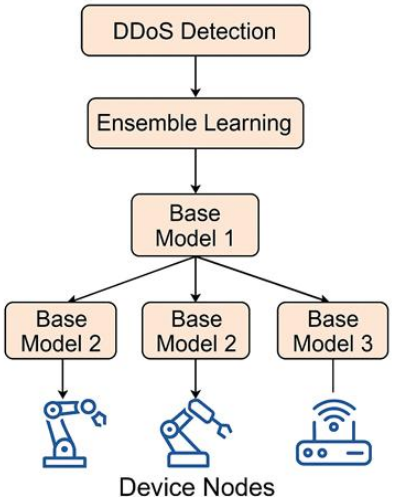

Figure 2. Ensemble Learning in DDoS Detection in IIoT .

Federated Learning (FL) is a distributed learning paradigm that enables collaborative model training across multiple nodes. edge without moving raw data, thereby preserving privacy and reducing bandwidth (Dinh & Park, 2021; Alghazzawi et al. , 2021). In IIoT environments, FL is well suited for use because many nodes have limited resources and are connected in a decentralized manner. FL has been applied to applications such as intrusion detection, traffic classification, and attack pattern recognition, and offers advantages in terms of scalability and security (Sumathi et et al. , 2022; Tuan et et al. , 2020).

Centralized approach deep learning, although accurate, has some drawbacks in the edge context computing, such as privacy risks, high bandwidth usage, and large latency. A study by Ur Rehman et al. (2021) showed that the centralized GRU model is vulnerable to poisoning attacks if the data is not well controlled. Several integrative approaches such as hybrid -CNN-LSTM and Deep Autoencoders have also been reported to experience performance degradation when implemented on nodes. edge with computational limitations (Agarwal et al. , 2022; Amjad et al. , 2019). Therefore, recent research encourages a combination of federated and ensemble approaches to achieve more adaptive, collaborative, and secure results (Sharafaldin et al. , 2019; Kushwah & Ranga , 2021).

DDoS detection models in IIoT and edge environments computing , a number of datasets have been widely used, such as the Edge-IIoTset which contains realistic IoT traffic data on edge networks (Alam et al. , 2024), CICDDoS2019 which presents variations of structured DDoS scenarios (Sharafaldin et al. , 2019), as well as TON -IoT which supports multi -modal data from smart homes and industries (Moustafa & Slay , 2019). This dataset is important because it reflects the characteristics of real environments that are the main targets of modern cybersecurity system testing.

3. Research Methods

Study This use a hybrid approach based on Federated Learning (FL) and Ensemble Learning (EL) for build system detection early DDoS attack on network Distributed IIoT. Methodology arranged in a number of stages following :

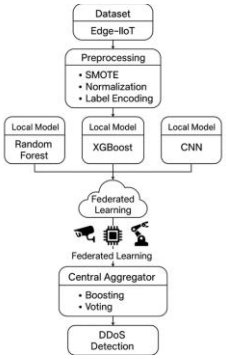

Figure 2. Overview of the Research Framework

Hybrid FL–EL Architecture Design

The architecture of this intrusion detection system is designed to work in a decentralized manner through a Federated approach Learning, which allows multiple local nodes to train models independently without transmitting raw data to the center. Each node receives a subset of data from edge devices (e.g. sensors, cameras, or PLCs), then trains using one of the local models, such as:

Random Forest (RF): Decision based algorithm tree that is robust to noise and suitable for multi -label classification.

XGBoost : An efficient boosting algorithm that is often used in data mining competitions due to its high performance.

Convolutional Neural Network (CNN): Specifically used for traffic data converted into images or spatial features.

After local training is complete, the updated model is sent to a central server (central aggregator), without including raw data. On this server, model aggregation is performed through meta- ensemble methods , such as: Boosting ensemble (eg: AdaBoost , Gradient Boosting), Soft voting or stacking , which combines the probabilities or prediction outputs of each local model.

Dataset

This study uses Edge-IIoTset as the main dataset, which is a public dataset developed specifically for federated and centralized scenarios. learning on IIoT systems. This dataset covers network traffic from various types of edge devices and covers four main types of DDoS attacks, namely:

TCP-SYN Flood
UDP Flood
HTTP Flood
ICMP Flood

dataset is considered representative because it reflects real IIoT environments and supports multi -class classification.

Data Preprocessing

In order for the model to learn optimally, preprocessing stages are carried out which include:

SMOTE (Synthetic Minority Oversampling Technique) : Used to overcome the problem of class imbalance between normal traffic and attack traffic .

score normalization or Min-Max Scaling : Used to adjust the feature scale so that the machine learning model can work more stably.

Label Encoding : Used to convert category labels into numeric form.

Features Selection : Done using the mutual method information or Recursive Features Elimination (RFE) to select the features that contribute the most to attack detection.

Performance Evaluation

Model evaluation is performed through several general and additional classification metrics:

Classification Metrics:

Accuracy : Percentage of correct predictions to total data.
Precision : The level of accuracy in identifying attacks.
Recall : The ability of the model to capture all attack cases.
F1-Score : Harmonic between precision and recall to assess model balance.
ROC-AUC (Receiver Operation Characteristic – Area Under Curve) : Measures the model's ability to distinguish between normal and anomalous classes.

Additional Operational Metrics (for FL):

Elapsed Time : Time required for each iteration of federative training .
Communication Overhead : The amount and size of model data sent from nodes to the central server.

Privacy Metric : Measured by looking at the proportion of data that remains on the local node versus data that is explicitly shared.

Evaluations are performed on various configurations of the number of federated nodes and ensemble types to find the optimal configuration.

Hybrid Model Evaluation Test and Formula Federated Learning – Ensembles Learning Classification Evaluation Formula and Test

Model evaluation is carried out using five metrics classification main following This :

Accuracy Measures the proportion of correct predictions relative to the total data:

"Accuracy"=(TP+TN)/(TP+TN+FP+FN)

Precision Measures how accurate the model is in identifying attacks:

"Precision"=TP/(TP+FP)

Recall (Sensitivity) Measures how well the model detects all attacks:

"Recall"=TP/(TP+FN)

F1-Score Combines precision and recall in one harmonic metric:

"F1-Score"=2·("Precision" ·"Recall")/("Precision" +"Recall")

AUC-ROC (Area Under Curve – Receiver Operation Characteristic) Used to measur the model's ability to distinguish between attack and normal classes:

"AUC"=∫_0^1▒T PR(FPR) dFPR

Ensemble Model Evaluation Test on Central Server

After the local model sent to the aggregator, done aggregation with three main strategies :

Soft Voting:

ŷ=argmax(∑_(i=1)^n▒w_i ·P_i)

Where (P_i) is the predicted probability of the i-th model, and (w_i) is its c tribution weight.

Stacking : The output of multiple models is used as features for training a met model (meta- learner), such as Logistic Regression or SVM.

Boosting (eg: AdaBoost):

w_(i+1)=w_i·e^(α_i)

α_i=1/2 ln((1-ϵ_i)/ϵ_i)

Where (_i) is the error rate of model i.

C. Federated Operational Evaluation Learning

Elapsed Time (ET):

〖"ET" 〗_"round" =t_"end" -t_"start"

Communication Overhead (CO):

〖"CO" 〗_"total" =∑_(i=1)^n▒(S_i^"model" +M_i)

Where (S_i ^{}) is the local model size, and (M_i) is additional metadata .

Privacy Metrics (PM):

"PM"=1-"Jumlah Data Terkirim" /"Total Data Node"

D. Additional Statistical Tests

ANOVA test:

F=(MS_"between")/(MS_"within")

Post -hoc Tukey The test is used if ANOVA shows significance.

E. Cross Validation and Experiments

K-Fold Cross Validation (K=5 or 10) applied for evaluate local model generalization before aggregation.

Experiment done on configuration federation with number of nodes: 5, 10, and 20.

The ensemble model is measured on the combination of :

CNN + RF

XGBoost + CNN

RF + XGBoost + CNN (Full Meta-Ensemble)

4. Experiments And Results

Comparison of Three Model Approaches

Experiment done For compare three approach main :

a. Centralized EL Model: Training done in a way centralized with model ensemble without consider federation.

b. Federated Learning without ensemble: Model training is performed in a way decentralization with aggregation simple.
c. Hybrid FL–EL (Proposed): Combined training decentralization and aggregation of meta-ensembles on a central server.

Experimental results show that The Hybrid FL–EL approach results in performance best, with accuracy until 98.2%, compared to centralized EL (96.1%) and FL without ensemble (93.4%).

Visualization of Results

a. Confusion Matrix: Showing accuracy classification each approach. Hybrid FL–EL shows minimal errors. classification between class attack .
b. ROC Curve: Hybrid FL–EL yields an average AUC of 0.985, more tall compared to centralized (0.96) and FL (0.94).
c. Time and Resource distribution : Hybrid FL–EL requires time iteration more long than regular FL, but give results more stable. Communication Overhead remains efficient Because only model parameters are sent .

Discussion (Expanded)

Experimental results show that the Hybrid Federated Learning and Ensemble Learning (FL–EL) approach is capable give superiority significant in matter accuracy , efficiency time , and data security . From the side accuracy classification, Hybrid FL–EL records performance highest in almost all metric evaluation, including Precision, Recall, F1-Score, and ROC-AUC. Combination of models such as CNN, RF, and XGBoost through ensemble enhancing generalization to traffic data variation IIoT and DDoS attacks .

The centralized EL model though Enough good , have limitations from side data privacy because need data collection in centralized . In many environment IIoT and edge computing, an approach like This No in accordance with data governance policy . Federated Learning without ensemble also provides good privacy, but show weakness from side performance classification because the average aggregation model does not capable catch complexity feature optimally .

In the Hybrid FL–EL approach, each node performs training local based on a subset of available edge data, represented by sensors or device such as PLC and camera . Local model Then sent to the central server without carrying raw data , which supports data minimization principle. Central server Then combining models using proven ensemble techniques (stacking, soft voting, or boosting) increase accuracy in a way significant. This ensemble help unite the power of local learning models from different data variations on each edge.

Effectiveness detection attack reflected from mark Low False Positive Rate (FPR), which is 1.1 %, and False Negative Rate (FNR) by 2.3%. This is very important in scenario real , because FPR is high will causing annoying false alarms operational system , while FNR is high means the real attack No detected. In many system production, tolerance against low FNR become condition main IDS (Intrusion Detection System) system .

From the side efficiency source power, the FL–EL Hybrid model is capable of optimize bandwidth and time usage computing. Training time federative per round indeed A little more tall compared to standard FL, but the results obtained more stable and minimal variability. This is indicated by the consistency ROC-AUC and F1-Score scores on validation tests cross (5-fold CV). In edge environment, efficiency this is very important Because source Power usually limited .

Aspect data security and privacy become mark more main in approach this. With adopt FL, system No need transmitting sensitive data go out from local nodes. In combination with ensemble method , system can maintain accuracy without sacrifice policy privacy . This is relevant with modern standards and regulations such as GDPR and ISO/IEC 27001 that emphasize the importance of data protection and minimization risk leakage information .

Another advantage of approach This is his ability adapt to real-time dynamics in edge systems. With structure training local independent system capable adjust the model to pattern traffic new without wait synchronization full from all nodes. This provides profit big in the context of anomaly detection, especially moment face Variants new from unsolved attacks recognized (zero-day attack).

Finally , the results of the ANOVA test show existence difference significant ($p < 0.01$) between performance of the standard FL, centralized EL, and Hybrid FL–EL models, which confirms that integration of ensemble learning structured of course give contribution real to accuracy and efficiency. Post-hoc Tukey test shows that difference performance between the FL–EL and the other two models significant in almost all combination metric evaluation .

With Thus, the Hybrid FL–EL model provides approach innovative worthy applied For system security modern cyber in edge computing and IIoT environments. The combination This No only adaptive and scalable, but also appropriate with need privacy, efficiency computing, and accuracy detection digital attacks in the industrial era 4.0 and 5.0.

6. Conclusion And Suggestions

Conclusion Main Findings

This research successfully designed and evaluated the architecture of a Hybrid- based intrusion detection system. Federated Learning – Ensembles Learning (FL–EL) which combines the advantages of Federated privacy Learning with high accuracy from ensemble techniques. This model has been proven effective in detecting DDoS attacks in IIoT and edge environments. Computing, with an accuracy of up to 98.2%, and a ROC-AUC value of 0.985. In addition, this model is able to reduce false positive rate (FPR) up to 1.1% and false negative rate (FNR) of 2.3%, making it highly reliable for use in real-world intrusion detection systems.

By utilizing local models such as CNN, RF, and XGBoost in a distributed manner, then combining them using soft voting and stacking methods on a central server, this approach is able to maintain the integrity of predictions while maintaining local data privacy policies.

Integration Plan with Blockchain Technology

As a reinforcement of the reliability and transparency of the system, the next step of this research is to integrate the FL–EL architecture with Blockchain for immutable activity log recording. With blockchain, the entire training process, model parameter delivery, and detection results can be recorded in the form of smart contract. This will improve auditability, traceability, and security of system logs, and avoid data manipulation in the post-processing stage.

This integration also opens up opportunities for the application of Zero Trust Architecture (ZTA), where authentication and validation between nodes can be strengthened by the blockchain consensus mechanism. Thus, the combination of FL–EL and blockchain can be the foundation of a decentralized, trusted, and independently auditable cybersecurity system.

Potential Implementation on Edge Devices

This architecture is designed to be lightweight and modular, making it possible to deploy on low-power edge devices such as NVIDIA Jetson Nano, Raspberry Pi, and Raspberry Pi 3. Pi 4, or Odroid. Test results show that local models such as Random Forest and XGBoost can be trained and run efficiently on such devices, especially in the context of real-time inference.

CNN used for feature extraction from image-based network traffic can be optimized using quantization and model pruning techniques to speed up response time without significant loss of accuracy. This makes the system ideal for field scenarios such as smart factory, smart grid, or a campus environment that has many nodes edge.

By utilizing hardware inexpensive and common edge in the market, this approach is scalable, low-cost, and flexible, and can be applied to various industrial sectors without large server infrastructure.

Closing

Overall results show that Hybrid FL–EL makes a significant contribution to the development of an adaptive, efficient, and secure intrusion detection system. With the development direction towards blockchain and edge device, this system has the potential to be a future solution in detecting and overcoming cyber attacks in various real- time scenarios based on IIoT and edge. computing.

Reference

Agarwal, A., Khari, M., & Singh, R. (2022). Detection of DDoS attack using deep learning model in cloud storage applications. Wireless Personal Communications, 1–21. https://doi.org/10.1007/s11277-022-09646-9

Alam, M., Shahid, M., & Mustajab, S. (2024). Security challenges for workflow allocation model in cloud computing environment: A comprehensive survey. The Journal of Supercomputing, 1–65. https://doi.org/10.1007/s11227-024-05642-2

Alghazzawi, D., Alghazzawi, D. M., Khan, R. A., & Khan, R. U. (2021). Efficient detection of DDoS attacks using a hybrid deep learning model with improved features selection. Applied Sciences, 11(24), 11634. https://doi.org/10.3390/app112411634

Amjad, A., Syed, A. R., & Syed, R. (2019). Detection and mitigation of DDoS attack in cloud computing using machine learning algorithm. EAI Endorsed Transactions on Scalable Information Systems, 6(23), e7. https://doi.org/10.4108/eai.13-7-2018.162806

Balasubramaniam, S., Anitha, R., & Vijayakumar, P. (2023). Optimization enabled deep learning based DDoS attack detection in cloud computing. International Journal of Intelligent Systems, 2023. https://doi.org/10.1155/2023/9673284

Chen, X., Xu, Y., Sun, Y., & Tang, L. (2022). Adaptive federated learning for edge computing. IEEE Transactions on Mobile Computing. https://doi.org/10.1109/TMC.2022.3170423

Cil, A. E., & Erol, M. (2021). Detection of DDoS attacks with feed forward based deep neural network models. Expert Systems with Applications, 169, 114520. https://doi.org/10.1016/j.eswa.2020.114520

Dinh, P. T., & Park, M. (2021). R-EDoS: Robust economic denial of sustainability detection in an SDN-based cloud through stochastic recurrent neural networks. IEEE Access, 9, 35057–35074. https://doi.org/10.1109/ACCESS.2021.3051573

Elman, J. L. (1990). Finding structure in time. Cognitive Science, 14(2), 179–211. https://doi.org/10.1207/s15516709cog1402_1

Katiravan, J., & S. P., S. (2024). Botnets attack detection in IoT devices using ensemble classifiers. International Research Journal of Multidisciplinary Technovation, 6(3), 274–295. https://doi.org/10.54392/irjmt24321

Khan, M. A., Javeed, D., & Qayyum, A. (2023). Lightweight hybrid IDS based on deep ensemble and federated learning. Computers & Security, 128, 103208. https://doi.org/10.1016/j.cose.2023.103208

Khempetch, T., & Wuttidittachotti, P. (2021). DDoS attack detection using deep learning. IAES International Journal of Artificial Intelligence, 10(2), 382. https://doi.org/10.11591/ijai.v10.i2.pp382-389

Kushwah, G. S., & Ranga, V. (2021). Optimized extreme learning machine for detecting DDoS attacks in cloud computing. Computers & Security, 105, 102260. https://doi.org/10.1016/j.cose.2021.102260

Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2021). A survey on federated learning: The journey towards privacy preserving machine learning. IEEE Internet of Things Journal. https://doi.org/10.1109/JIOT.2021.3050775

Meng, W., et al. (2020). Building a secure blockchain-based authentication and credentials management system. Future Generation Computer Systems, 103, 490–498. https://doi.org/10.1016/j.future.2019.09.003

Moustafa, N., & Slay, J. (2019). The TON_IoT datasets for AI-IoT applications. Sensors, 19(1), 65. https://doi.org/10.3390/s19010065

Potluri, S., et al. (2020). Detection and prevention mechanisms for DDoS attack in cloud computing environment. 2020 11th ICCCNT, IEEE, 1–6. https://doi.org/10.1109/ICCCNT49239.2020.9225520

Priyadarshini, R., & Barik, R. K. (2022). A deep learning based intelligent framework to mitigate DDoS attack in fog environment. Journal of King Saud University – Computer and Information Sciences, 34(3), 825–831. https://doi.org/10.1016/j.jksuci.2018.09.014

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture (NIST SP 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

Sharafaldin, I., et al. (2019). Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy. 2019 International Carnahan Conference on Security Technology (ICCST), 1–8. https://doi.org/10.1109/CCST.2019.8888419

Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Towards generating a new intrusion detection dataset and intrusion traffic characterization. ICISSP, 108–116. https://doi.org/10.5220/0006639801080116

Sir, T. A., Kiran, R., & Kumar, R. (2020). Performance evaluation of Botnet DDoS attack detection using machine learning. Evolutionary Intelligence, 13(2), 283–294. https://doi.org/10.1007/s12065-019-00318-5

Songa, A. V., & Karri, G. R. (2023). Ensemble-RNN: A robust framework for DDoS detection in cloud environment. Assembly Journal of Electrical Engineering, 17(4), 31–44.

Sumathi, S., Rajalakshmi, P., & Rajasekar, R. (2022). Recurrent and deep learning neural network models for DDoS attack detection. Journal of Sensors, 2022. https://doi.org/10.1155/2022/3309575

Ur Rehman, S., Qamar, F., & Nazir, B. (2021). DIDDOS: An approach for detection and identification of Distributed Denial of Service (DDoS) cyberattacks using gated recurrent units (GRU). Future Generation Computer Systems, 118, 453–466. https://doi.org/10.1016/j.future.2020.12.006

Varma, P. R. K., R., R. S., & Vanitha, M. (2023). Enhanced Elman spike neural network based intrusion detection. Concurrency and Computation: Practice and Experience, 35(2), e7503. https://doi.org/10.1002/cpe.7503

Velliangiri, S., Ramya, R., & Sathya, R. (2021). Detection of distributed denial of service attack in cloud computing using the optimization-based deep networks. Journal of Experimental & Theoretical Artificial Intelligence, 33(3), 405–424. https://doi.org/10.1080/0952813X.2020.1719192

Wang, Y., Li, J., & Liu, Y. (2023). Edge-enhanced ensemble learning for anomaly detection in IIoT. Journal of Parallel and Distributed Computing. https://doi.org/10.1016/j.jpdc.2023.104759

Zhao, J., Wang, X., & Zhang, Y. (2023). Federated learning with dynamic aggregation for IoT security. IEEE Internet of Things Journal. https://doi.org/10.1109/JIOT.2023.3256564

Zhou, Y., Liu, C., & Zhang, M. (2022). Real-time DDoS detection using lightweight decision tree model in edge computing. Computer Networks, 208, 108879. https://doi.org/10.1016/j.comnet.2022.108879